Information Technology (IT) Initiative
Business Case Responses for BYs 2003 & 2004

Please type your responses in the white answer blocks provided and return the electronic copy of this document to Treva Lutes by April 26th. Please do not modify the shaded rows of the table. These rows contain special codes that we will use to populate a database automatically.

1.0 General Background

1.1 Initiative Name

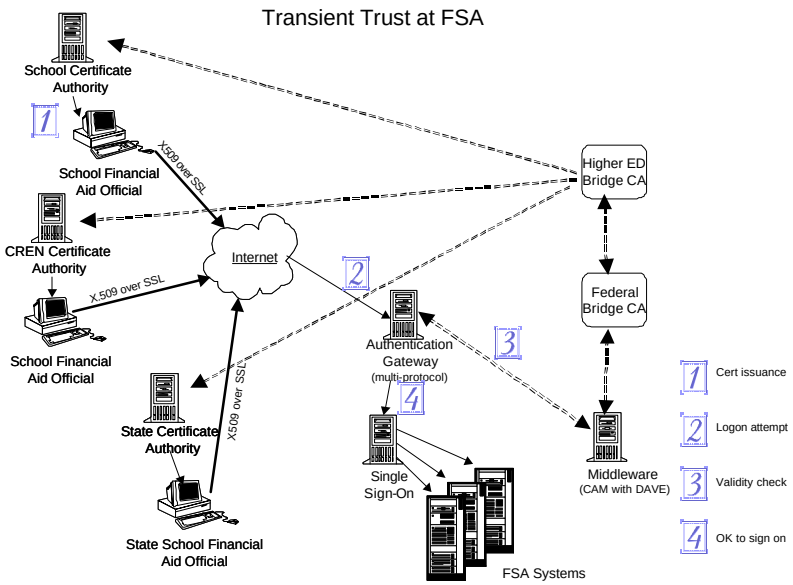
FSA Single Sign-On

1.2 Initiative Description

Under the current FSA systems architecture, users in FSA partner organizations (schools, guaranty agencies, lenders, servicers, and state agencies) must use separate logon credentials (user IDs and passwords) to access each FSA system needed to perform their duties. In addition, as new and modernized systems are released, these users may require additional usernames and passwords.

The Single Sign-on initiative reduces the number of usernames and passwords users need to remember to access FSA systems and creates a secure technology infrastructure for logging users in and out of the FSA systems they are authorized to access. The initiative also provides for a common system enrollment process regardless of which FSA system users require access. This result provides FSA with a more secure identification and authentication process while providing FSA's customers with a simpler method to do business with FSA. This enhancement to the FSA systems infrastructure helps FSA accomplish its performance goal of to building and operating systems worthy of trust.

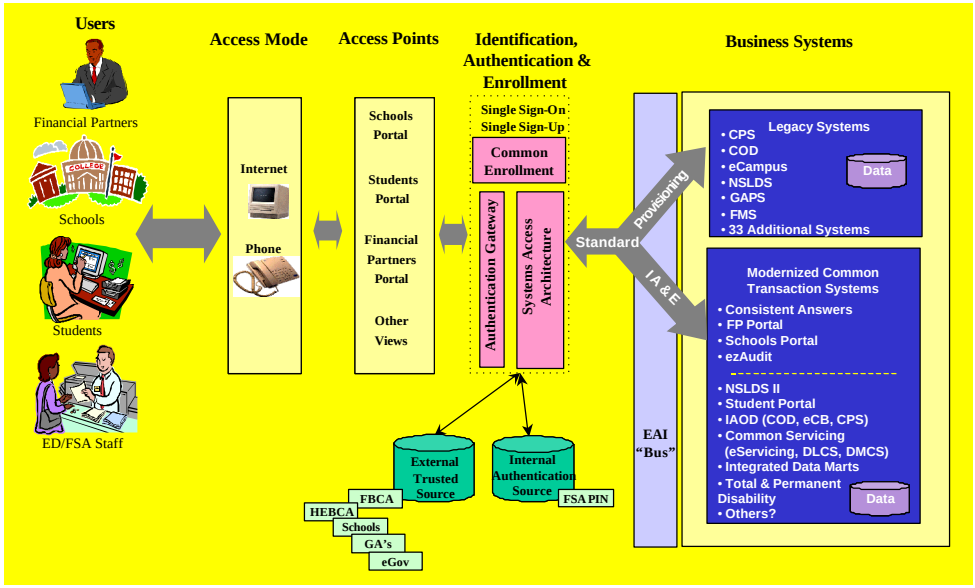
This effort enables FSA to participate with the federal e-authentication initiative, as part of the President's e-Gov agenda, by providing a business infrastructure which links to services. E-Authentication is substantiated within FSA vision of "Transient Trust"; this vision sees users being authenticated by FSA's trusted business partners based on agreed to policies and standards:



The federal e-Authentication initiative envisions the following capabilities to be provided by organizations (Office of Electronic Government, Jan. 31, 2002):

- Single Sign on
- Access to multiple services
- Multiple Access levels - assurance commensurate with levels of risk
- Interoperable, scalable, secure

This scope of this initiative includes each of these capabilities. The following depicts the vision of the Single Sign On initiative, and its scope which encompasses FSA customer access points, existing and new business systems, linkages to external authentication mechanisms (i.e., sources of "transient trust"), and integration to the FSA PIN:



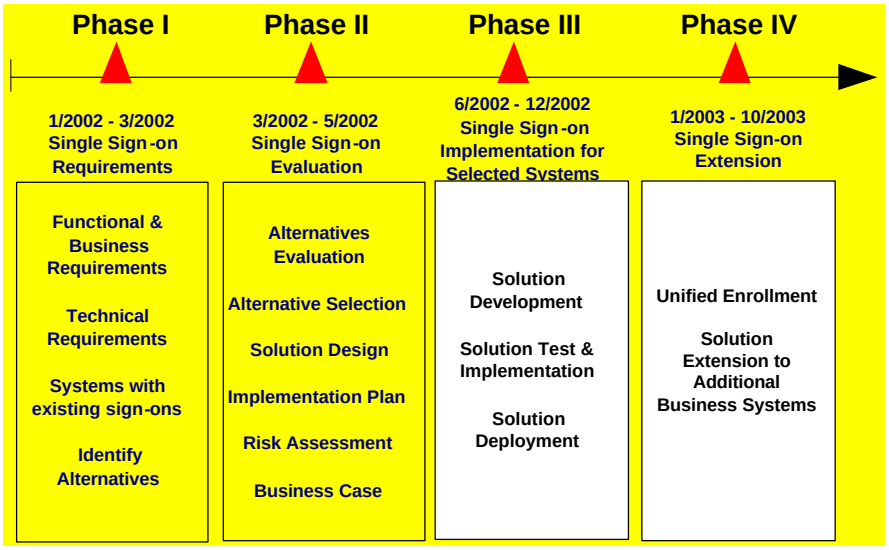
Phase I of this initiative, completed March 2002, identified business and technical requirements for an FSA Single Sign-On service. The requirements were compiled and recommended by an enterprise IPT (Integrated Product Team) and IPT advisory team. These requirements were compiled as a result of interviews conducted within FSA, industry and market research, and past efforts related to Single Sign-On services. The key requirements for an FSA

Single Sign-On service, as determined by this IPT, are that the single sign-on solution: Be web-based, Provide a high-level of availability, Integrate with the FSA PIN, Enhance FSA system access security, Provide a reusable solution, and Integrate with new and existing FSA business applications.

Phase II of this initiative, completed June 2002, completed a general design for FSA's Single Sign-On service for School, FSA employee, Financial Partner, and Student users of FSA systems. This design identified core business processes and application capabilities required, data flow definition, and a basic technology/network architecture each based upon the requirements identified during Phase I. In addition, then enterprise IPT completed an analysis of solution alternatives was completed; this analysis recommended that FSA establish an operational and technology infrastructure that provides a common identification and authentication (I&A) infrastructure for all systems to be modernized and future systems, provisioning capabilities for existing systems, and a common enrollment capability. The IPT team also completed a formal review of internal capabilities, GOTS/COTS providers, and service providers capable of meeting FSA's needs, and completed a high-level implementation plan based on vendor/service provider recommendation and requirements.

Phase III will complete the detailed design, development and deployment of a Single Sign-On service for selected FSA business applications. FSA will implement the basic infrastructure for its Single Sign-On service, as well as enabled selected new and/or legacy systems with this capability. This infrastructure will provide a capability for users to access FSA applications from FSA Portals or directly using a single login. This phase will also develop a basic user enrollment service for these selected systems.

The scope of Phase IV is to extend the basic infrastructure deployed during Phase III to further leverage the efficiencies in identity management. The following chart shows each phase of the single sign on effort:



This business case covers the continuation of the modernization development and deployment process that began in FY 2001. This phase involves deployment of the single sign-on capability to additional FSA partner-facing business systems, as well as more detailed requirements for user enrollment to FSA business systems.

1.3 Initiative Type

Business Process Support System
Financial Management System _____
Non-Financial Management System ____

Program Delivery System
Financial Management System _____
Non-Financial Management System _____

IT Infrastructure __X___
IT Services _____
General Office Automation _____

1.4 Contact Information

	Name	Principal Office	Phone Number
Project Manager	Neil Sattler	FSA	(202) 377-3513
Program Manager	Neil Sattler	FSA	(202) 377-3513
Project Sponsor	Steve Hawald	FSA	(202) 377-3501
Contracting Officer	Janet Scott	FSA	(202) 377-3377
Contracting Officer's Representative	Carol Seifert	FSA	(202) 377-3506

2.0 Business Process

2.1 Business Process Support

___ Grants
___ Evaluation
___ Research
_X_ Information Dissemination
___ Enforcement
___ Resource Management & Administration
___ Loans
_X_ Other: Information Security

The initiative currently supports modernization initiatives within the FSA enterprise for identity management of users across the channels. All future modernization initiatives will utilize the common identification and authentication service to provide access to FSA systems. Additionally, the modernized initiatives will utilize the common system enrollment service for the generation of identification and authentication. Specifically, the initiative will integrate with the Title IV participation management function to provide system enrollment services within the Schools and Financial Partners channels. The initiative will benefit the Students channel by allowing students to login once for transactions associated with multiple back-end systems. The initiative will support information dissemination and information security.

2.2 Business Problem or Opportunity and Causing Conditions

System users utilize multiple access credentials to logon to FSA systems, which may also have multiple and differing Channel-specific access points. In addition, as new and modernized systems are released, additional access credentials and rights may also be created. This could create increasing opportunities for unauthenticated access to FSA systems, undermining the credibility of FSA, and affecting its ability to help put America through school. The management of multiple user identities is administratively burdensome and costly to FSA and inconvenient to our customers.

2.3 Existing Systems

Each existing system has its own individual authentication and user login. Requirements from Phase I indicate that 39 separate authentication and user login schemes exist. The scope within the business case for Phase III includes the following new systems – ezAudit, Consistent Answers, School Portal, Financial Partners Portal – and the following critical existing systems - National Student Loan Data System (NSLDS), Grant Administration and Payment System (GAPS), Central Processing System (CPS), Common Origination & Disbursement (COD), and eCampus Based (eCB) - as candidate systems for the initial implementation of single sign-on.

Additional systems enabled within the single sign-on solution during Phase IV may include additional Schools, Students, and Financial Partners Channel partner-facing systems.

2.4 Solution Impact
(If this is an implemented initiative with no enhancements, then address item (3) only)

(1) The initiative impact will create a single login and enhanced security for login to FSA systems utilizing the common identification and authentication service as well as the common enrollment service.

- Improve customer access to FSA systems – provide a Common user identifier
- Strengthen cyber-security – provision a trusted user identifier

(2) The business drivers for a single sign-on service (and thus the areas it will impact) are to:

- Establish a reusable Single Sign-on service for FSA business systems:
- Existing FSA system users have multiple logins/passwords. A Single Sign-on solution will provide them with an easier and more efficient way to reach the data and tools they need to access.
- Modernization and integration efforts will implement additional logins without Single Sign-on services.
- Existing systems have their own enrollment processes for system access. This initiative provides for a common enrollment process to modernized systems.

(3) This initiative will directly benefit FSA employees, school financial aid administrators, students, and financial partners. Other stakeholders include the Department of Education as a whole and its goal to maintain electronic systems with the required level of security capabilities.

(4) This initiative has been developed in partnership with the affected FSA system program officers, and system security officers.

(5) The overall technical architecture and security framework for FSA is an integral part of this single sign-on solution. Internal and external users of FSA business systems will be trained and provided the opportunity to enable themselves to access with a single login those FSA systems in which they are enrolled.

2.5 Business Process Reengineering
(Applies only to New Business Process Support and Program Delivery Systems)

The new business process that will be supported use the following:

1. A user logs in once and receives seamless access to the services they are entitled to access without having to identify and authenticate him/herself multiple times. This effort was initiated in FY2002 with a planned implementation timeframe of December 2002. This business case supports the expansion of the Single Sign On solution to additional School and Financial Partner Channel partner facing systems.
2. A new process to enroll new users to systems that are Single Sign-On enabled. This process will provision a user's single sign-on access credentials, back-end system credentials, and obtain user profile data.

2.6 Mandatory Requirement

(1) As stated by OMB Circular A-130 (as updated 11/28/2000), Management of Federal Information Resources, Appendix III, Security of Federal Information Resources, "Ensure that appropriate security controls are specified, designed into, tested, and accepted in the application in accordance with appropriate guidance issued by NIST." for Technical Controls for identification and authentication
(2) As per NIST800-18, Guide for Developing Security Plans for Information Technology Systems (December 1998), Section 6.MA.1, Identification and Authentication, guidance "Identification and Authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. For example, access control is often based on *least privilege*, which refers to the granting to users of only those accesses minimally required to perform their duties. User accountability requires the linking of activities on an IT system to specific individuals and, therefore, requires the system to identify users."
(3) These requirements ask for a secure identification and authentication system for all applications.

2.7 Consequence of Not Funding the Initiative

If this effort is not funded, the following are the consequences FSA faces:

1. System by system user enrollment will continue.
2. System by system user identification will continue.
3. System by system user authentication will continue.
4. FSA will continue to build new identification and authentication sources for new and reengineered systems.
5. Users will have to remember multiple user IDs, passwords and other sign on credentials for multiple systems.
6. There will be continued security concerns with respect to the identity of our users and the potential compromise of access credentials.

3.0 Strategic Alignment

3.1 OMB E-Government Initiative Alignment

___Consolidated Health Information
___Disaster Assistance and Crisis Response
_X_E-Authentication
___E-Grants
___E-Payroll/HR
___E-Training
___E-Travel
___E-Vital
___Electronic Records Management
___Eligibility Assistance Online
___Expanding Electronic Tax Products for Businesses
___EZ Tax Filing
___Federal Asset Sales
___Federal Enterprise Architecture
___Geospatial Information One Stop
___Integrated Acquisition Environment
___Integrated Human Resources/e-Clearance
___International Trade Process Streamlining
___One Stop Business Compliance Information
___Online Access for Loans
___Online Rulemaking Management
___Recreation One Stop

___Recruitment One Stop
___USA Services
___Wireless Public Safety Interoperable Communications – Project SAFECOM
_ _None of the Above

3.2 Mission Alignment

- Goal 1: Create a Culture of Achievement
___ Objective 1.1 Link federal education funding to accountability for results.
___ Objective 1.2 Increase flexibility and local control.
___ Objective 1.3 Increase information and options for parents.
___ Objective 1.4 Encourage the use of scientifically based methods within federal education programs.

- Goal 2: Improve Student Achievement
___ Objective 2.1 Improve reading achievement for all students.
___ Objective 2.2 Improve math and science achievement for all students.
___ Objective 2.3 Improve the performance of all high schools.
___ Objective 2.4 Improve teacher quality.

- Goal 3: Develop Safe Schools and Strong Character
___ Objective 3.1 Ensure that our nation's schools are safe and drug-free and that students are free of alcohol, tobacco, and other drugs.
___ Objective 3.2 Promote strong character and citizenship among our nation's youth.

- Goal 4: Transform Education into an Evidence-Based Field
___ Objective 4.1 Raise the quality of research funded or conducted by the Department.
___ Objective 4.2 Increase the relevance of our research in order to meet the needs of our customers.

- Goal 5: Enhance the Quality of and Access to Postsecondary & Adult Education
___ Objective 5.1 Close the college participation and graduation gaps between low-income and minority students and their peers.
___ Objective 5.2 Strengthen accountability of postsecondary institutions.
___ Objective 5.3 Establish effective funding mechanisms for postsecondary education.
___ Objective 5.4 Strengthen Historically Black Colleges and Universities, Hispanic Serving Institutions, and Tribal College and Universities.
___ Objective 5.5 Enhance the literacy skills of American adults.

- Goal 6: Establish Management Excellence
_X_ Objective 6.1 Develop and maintain financial integrity within the Department and its programs and management and internal controls.
___ Objective 6.2 Improve the strategic management of the Department's human capital.
_X_ Objective 6.3 Manage information technology resources, using e-gov, to improve service for our customers and partners.
_X_ Objective 6.4 Continue to modernize the Federal Student Aid (FSA) Assistance programs and reduce their high-risk status.
___ Objective 6.5 Achieve budget and performance integration to link funding decisions to results.
___ Objective 6.6 By demonstrating management excellence, receive the prestigious President's Quality Award.

___**None of the Above**

3.3 Strategic Plan Strategies Supported

Objective 6.1 Develop and maintain financial integrity and management and internal controls.

Update and integrate financial systems. We will implement a new financial system capable of producing timely and reliable financial data and reconcile systems to the general ledger.

Prepare financial statements to provide leading data on Department performance. The Department will create quarterly financial statements to track financial performance against agreed upon budgets.

Analyze data to reduce fraud. The Department will create data analysis capabilities within financial and program management systems and will refer any cases of suspected fraud to the Inspector General's office.

Review existing internal controls and implement changes where necessary. These efforts will include processes for monitoring and holding grantees, contractors, guarantors and lenders accountable and closing open audit recommendations.

Increase the use of performance-based contracting. Contractors will be held accountable to objective performance criteria.

Objective 6.3 Manage information technology resources, using e-gov, to improve services for our customers and partners.

Encourage customers to conduct business with the Department on-line. The Department will implement productivity improvements through implementation of e-gov applications, customer relationship management, supply chain management, and knowledge management best practices, while at the same time protecting the privacy of our customers.

Ensure security of the IT infrastructure. We will periodically update and validate the General Support Systems (GSS) and Major Applications (MA) Inventory. For each GSS and MA, assure a current risk assessment and security plan and that certification and accreditation are in place.

Reduce our partners' data reporting burden. The Department will minimize burden on our partners and improve the quality of federal data by implementing a performance-based data management initiative. We will collect data once and use it in many ways. We will consolidate our data collections and data storage. With our stakeholders and customers, we will collaboratively build and publish data standards, including consensus data elements and definitions. The enterprise architecture will be structured to meet business needs. (See Objective 1.2 for more on this topic.)

Complete enterprise architecture. The Department will create a business-focused enterprise architecture that describes long-term information system requirements and prioritizes IT business needs based on Strategic Plan Goals and Objectives.

Objective 6.4 Modernize the Student Financial Assistance programs and reduce their high-risk status

Create an efficient and integrated delivery system. We will use new technologies and integrate systems by eliminating, consolidating, and redesigning the thirteen current legacy systems to improve service, cut costs and reduce the improper payment of student aid funds.

Improve program monitoring. The Department will strengthen financial management and internal controls so that relevant, timely information is available to manage day-to-day operations. We will improve technical assistance

and increase program monitoring.

3.4 Quality Indicators

The success of the initiative will be determined by the following quality indicators:

- The number of users having single sign-on IDs (number of FSA system users having a “single sign-on” access credential).
- Reduced system help desk support for login related questions (decreased number of calls to system help desks for username lookup and password change/reset needs).
- Increase in customer satisfaction from not having to enroll in multiple systems (fewer system enrollment processes, availability of a single, common enrollment service for “single sign-on” enabled systems).
- Increase in customer satisfaction from not having to use multiple logins to access FSA systems (reduction in the number of credentials a user requires to access FSA systems).
- Decreased development time since the identification and authentication service as well as the enrollment service will be reused (availability of a single, common access control capability for new and reengineered FSA systems).
- Faster processing for enrollment of new FSA system users (availability of a single, common enrollment service for “single sign-on” enabled systems).
- Better access to FSA systems leading to customer satisfaction and user happiness (reduction in the number of credentials a user requires to access FSA systems).
- Better security with a standard identification and authentication service for modernized FSA systems (fewer calls to system help desks for username lookup and password change/reset needs).
- Increase in maintainability due to the reusable and central nature of the identification and authentication and enrollment service (availability of a single, common access control capability for new and reengineered FSA systems).

4.0 Technology Initiative

4.1 Initiation Date

January 31, 2002

4.2 Initiative Deployment / Implementation Date

Initial Deployment: December 31, 2002
Extended Deployment: September 30, 2003

4.3 Initiative Phase

__X__ Under Development
_____ Maintenance Only
_____ Maintenance with Enhancements

4.4 Initiative Scope

The scope of this effort is to:

1. Expand the deployment of a standard Identification and Authentication service to additional partner facing business systems for users accessing these applications through the Schools, Financial Partners and Students Channels.
2. To define and approve requirements for user participation and enrollment to FSA systems. A common approach to system enrollment for those systems required for participating in FSA Title IV and other programs critical to the management of student aid will be developed. This approach will include links to participation management and quality assurance as necessary to ensure that only qualified users are provided access to FSA business applications.

The work services covered during this effort are:

- Requirements definition and analysis
- General Design
- Development
- Deployment

The milestones associated with Phase IV of this initiative further leverage the infrastructure established within the earlier phase III (Initial Deployment). Further, Phase IV expands upon the requirements activities performed during Phase I (Requirements) and Phase II (Alternative Assessment). Specifically, as additional modernization initiatives are undertaken, the service will be reused and result in quicker deployment of modernization initiatives at lesser cost.

4.5 Assumptions, Constraints, and Dependencies

(1) It is assumed that the FY2002 implemented Single Sign On solution will be expanded in FY2003 and enable other FSA legacy and modernized systems to reduce their efforts to implement an e-authentication solution.
(2) N/A
(3) The systems that will be initially served through the single sign-on effort, upon approval of Phase III, will be selected from the following new systems – ezAudit, Consistent Answers, School Portal, Financial Partners Portal – and from the following critical existing systems - Common Origination and Disbursement System (COD), the Central Processing System (CPS), eCB, FMS, NSLDS and GAPS.

4.6 Outstanding Issues

1. Additional systems to be included in the Single Sign On Phase IV expansion have yet to be finalized.
2. The requirements for unified (single point of) participation and enrollment have not been defined.
3. Multiple help desks (customer support) for single sign-on enabled applications/systems; relationship has not been coordinated with the consistent answers initiative.
4. The sequencing plan, or implementation plan, for enabling all FSA systems with single sign-on capability has not yet been determined.

4.7 Benefits

FSA Single Sign-On could provide the following benefits:

- Improved customer access to FSA systems
- Support the web-based access needs for FSA's Portals and overall eCommerce strategies
- Strengthened cyber-security by using a trusted identifier
- Establish a reusable Single Sign-on service for FSA systems
- Provide potential future economic savings
- System enrollment
- User access management
- Reduced customer support for login

4.8 Crosscutting Initiative

___ Entire Department
___ Office for Civil Rights
___ Office of Educational Research and Improvement
___ Office of Elementary and Secondary Education
___ Office of English Language Acquisition
___ Office of Postsecondary Education
___ Office of Special Educational and Rehabilitation Services
_X_ Federal Student Aid
___ Office of Vocational and Adult Education
_X_ Office of the Chief Financial Officer (GAPS)
_X_ Office of the Chief Information Officer (EDNET)
___ Office of the General Counsel
___ Office of Inspector General
___ Office of Intergovernmental and Interagency Affairs
___ Office of Legislation and Congressional Affairs
___ Office of Management
___ Office of Public Affairs
_X_ Entities outside of the Department

4.9 Audit Finding

None

4.10 Alternatives Analysis
(This Applies Only To Initiatives Under Development or Being Implemented.)

Alternatives	Description	Total Life Cycle Costs	Benefits	Drawbacks
Alternative 1 (Selected Alternative) *Expand Single Sign-On*	Expand the deployment of Single Sign-On; Determine participation and enrollment requirements	FY2002: $3M FY2003: $2.45M FY2004-07: $5.5M (Operations) Total: $11M	Listed above in section 4.7. Additionally, this initiative will provide the technology compatible with the evolving eAuthentication standards.	Additional systems will need to be single sign-on enabled to present customers with single login capability to all FSA system privileges. No drawbacks to the requirements phase of participation and enrollment.
Alternative 2 *No Single Sign-On Expansion*	No further deployment	$3.0M funded to date (the end of FY2002)	Infrastructure for and enterprise single sign-on solution deployed for future expansion.	Limited utility for customers and employees.
Alternative 3	N/A.			
Alternative 4				

The selected alternative, the expansion of Single Sign On, was selected as it meets Department goals relating to improved customer and employee satisfaction and reduction of unit costs. This initiative also supports the Department's Strategic Plan and the President's e-gov agenda.

5.0 Enterprise Architecture

5.1 Use of COTS/GOTS

	Percentage of COTS/GOTS Components: ___ 0 - 25% ___ 26 - 50% _X_ 51 - 75% ___ 76 - 100% ___ Not Applicable

5.2 Consistency with Product Support Plan
(Please refer to Appendix A to identify supported products and indicate non-supported products below)

Utilizes supported products as implemented in Single Sign-On Phase III. Vendor selection and product review is currently in process.

5.3 Section 508 Compliance
(Accessibility)

(1) No. The project has not yet been implemented
(2) No. The project has not yet been implemented.
(3) All software will be made available to people with disabilities. Once hardware and software for this initiative is selected and designed, support from the Department's Assistive Technology team will be required to ensure Section 508 compliance.

5.4 Government Paperwork Elimination Act (GPEA)
(Business Process Support and Program Delivery Systems only)

N/A

5.5 Information Management
(Business Process Support and Program Delivery Systems only)

N/A

5.6 Privacy

This initiative will not collect and maintain personally identifiable information, such as names, social security numbers, home addresses, or other personal identifiers.

5.7 Security
(This question applies if the initiative meets the definition of major application or general support system as defined in OMB Circular A-130.)

Part 1 – a. (Please enter a date in the form of MM/DD/YYYY or N/C)

January 15, 2002

Part 1 – b. (Please enter a date in the form of MM/DD/YYYY or N/A)

N/A
Part 1 – c.
N/A
Part 2 – a. (Please enter a date in the form of MM/DD/YYYY or N/C)
N/C
Part 2 – b. (Please enter a date in the form of MM/DD/YYYY or N/A)
10/31/2002
Part 2 – c.
Upon development. This is not an existing FSA system, and is not required to meet GISRA's reporting requirements this FY.
Part 3 – a. (Please enter a date in the form of MM/DD/YYYY or N/C)
N/C
Part 3 – b. (Please enter a date in the form of MM/DD/YYYY or N/A)
10/31/2002
Part 3 – c.
Upon development. Security plans of participating systems will also need to reflect new authentication capability resulting from this initiative. This is not an existing FSA system, and is not required to meet GISRA's reporting requirements this FY.
Part 4 – a. (Please enter a date in the form of MM/DD/YYYY or N/C)
N/C for 2002
Part 4 – b. (Please enter a date in the form of MM/DD/YYYY or N/A)
06/30/2002
Part 4 – c.
Upon development. This is not an existing FSA system, and is not required to meet GISRA's reporting requirements this FY. Self-Assessments should be completed during June of the first year of operation.
Part 5 – a. (Please enter a date in the form of MM/DD/YYYY or N/C)
N/C
Part 5 – b. (Please enter a date in the form of MM/DD/YYYY or N/A)
04/31/2003
Part 5 – c.
Upon development. Our C&A documentation will be completed prior system implementation.
Part 6 – a. (Please enter a date in the form of MM/DD/YYYY or N/C)
N/C
Part 6 – b. (Please enter a date in the form of MM/DD/YYYY or N/A)
04/31/2003
Part 6 – c.
Upon deployment. Our C&A documentation will be completed prior system implementation.

6.0 Risk and Project Management

6.1 Risk Management

Risk Category	Risk Description	Risk Probability	Risk Impact	Management Strategy
Strategic	The risk of not implementing the Single Sign-On initiative will lead to additional logins required by users, multiple redundant enrollment processes and thereby decrease customer satisfaction with FSA services. Single Sign-On is a component of the FSA Modernization Blueprint to provide increased customer service and a single identification and authentication standard for FSA applications. An appropriate standard for identification and authentication needs to be developed.	Low	Medium	Input from the Department, FSA, customers, industry groups and other Federal e-Gov initiatives will be included to ensure compatibility of the FSA single sign-on solution.
Organizational/Change Management	A lack of central management of the identification and authentication to our systems will lead to fragmented processes and increased vulnerabilities. This enterprise service function will need to be managed centrally by FSA.	Low	Low	Appropriate recommendations will be made at the conclusion of Phase III.

Project Resources (Financial, Personnel, etc.)	Within the Government, there is an increased emphasis on security requirements. This initiative provides a modernized basis for addressing security issues related to customer access to our systems. Security, Identification and Authentication, and single sign-on enabled system-specific authentication resources will be required to implement a successful solution.	Low	Medium	The project team will be comprised of resources knowledgeable on security, identification and authentication and FSA systems.
Project Management	As with all enterprise initiatives, coordination across multiple organizations – internal to and external to FSA will be key to success. The project will need coordination across all the life cycle stages as well as resources, technology, and applicable standards.	Low	Low	An IPT (Integrated Product Team) approach will be utilized to ensure timely participation and contribution.
	The sequencing plan, or implementation plan, for enabling all FSA systems with single sign-on capability has not yet been determined.	Low	Medium	For Phases III and IV of this initiative, an enterprise IPT will recommend to the FSA senior leadership which systems should be enabled. FSA channel GM's and the management council will specify the specific systems to be enabled and the implementation plan.

Business	Strengthening the identification and authentication and enrollment process will require close coordination with the customer community. The FSA customers will need to adopt this single sign-on solution for single login and access to FSA systems.	Low	Low	Phase III and Phase IV activities will include community outreach tasks to ensure comprehensive understanding of new service.
	Multiple help desks (customer support) for single sign-on enabled applications; relationship has not been coordinated with the consistent answers initiative.	Low	Medium	The project team will work with the consistent answers team to develop an integrated approach for single sign-on help desk support.
Data/Information	The fragmented access mechanisms to our systems lead to system vulnerabilities that can be controlled. Login data will be maintained within the appropriate single sign-on data store.	Low	Medium	The design of the login data store will include federal standard levels of encryption, backups for recovery and hot sites continuity of operations.
Application	A long-term vision for an architecture will need to be realized across all enterprise system assets. Connectors from single sign-on to FSA systems will be required.	Low	Low	Industry and Federal standard techniques will be utilized to implement COTS/GOTS connectors from the single sign-on facility to enabled systems.

Technology/Infrastructure	The single sign-on technology is maturing, the federal standards for cross-organization identification and authentication are evolving, and appropriate infrastructure will be required.	Low	Low	Phase III will implement technology compatible with the evolving e-Gov e-Authentication standards, PAMs (Pluggable Authentication Modules) to support additional identification and authentication sources and the infrastructure will be scaled to handle the required capacity.
Security	Login data will be maintained within the single sign-on data store to support single login.	Low	Medium	The design of the login data store will include federal standard levels of encryption, backups for recovery and hot sites continuity of operations.
Privacy	No privacy data will be collected.	N/A	N/A	N/A

6.2 Operational Performance Measures

Success will be achieved when the single sign-on solution is expanded to additional partner facing systems. During Phase III of this effort up to five systems will be enabled together with the deployment of an enabling infrastructure. During Phase IV up to five additional systems will be enabled; additional systems can be enabled based upon FSA direction.

Success will also be achieved when requirements for unified user participation and enrollment service are understood, documented and submitted. During Phase III a common enrollment service will be provided for single sign-on enabled systems. During Phase IV requirements will be identified for participation management and enrollment, and links to other FSA capabilities providing related participation management and enrollment services.

Ideally, a majority of partner facing systems would be integrated into the single sign-on system and all students, parents and partners would have single sign-on user names and passwords.

Specific outcomes will include increased customer satisfaction (measured by fewer system logins and decreased call volumes to system help desks for username changes and password changes/resets), decreased system access vulnerabilities (measured by the establishment of systems access credentials meeting NIST 800-18 technical control guidelines for identification and authentication - NIST800-18 Guide for Developing Security
Plans for Information Technology Systems, Section 6.MA.1 Identification and Authentication, “Identification and Authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system.”), and more efficient identification and authentication and enrollment processes (measured by the establishment of a standard and common systems access control capability, and establishment of common system enrollment capability for single sign on enabled systems) which are cheaper to maintain for compliance with industry and federal security standards.

6.3 General Acquisition Strategy

(1) Single Contract
(2) This initiative will be contracted as Firm Fixed Price contract with the FSA Modernization Partner. The contract type is a Blanket Purchase Agreement (BPA) under GSA Schedule 70 Contract (GS-35F-4692G) implemented using Task Orders (FP, FP Share in Savings IF, and T&M)
(3) N/A
(4) The contract lasts from 9/7/99 – 9/30/02 with two 5-year options. Task Order contract (#82) ends 5/17/02. Phase Three (Task Order 100) is expected to end 12/02. Phase IV is expected to start 1/03 and end 09/03.
(5) **Project:** Modernization Partner
Contract Type: BPA #: ED-99-DO-0002
(6) Complete an RFI where multiple sources of the single sign on service were evaluated. Each of the following business models was addressed: Custom development and operations by FSA, enhance an existing service (FSA PIN) and operate by VDC, purchase and integrate a COTS product and operate by FSA, purchase a managed service provider service which is integrated and operated by service provider.
(7) Phase II recommended a vendor from the RFI results and Phase purchased product/services from this vendor.
(8) Single Contract
(9) Fixed Price
(10) N/A

APPENDIX A

Hardware

Personal Computers

Primary Support

___Compaq Professional Pentium II (266 MHz or faster), minimum 64 MB of RAM, 3.0 GB of Hard Drive available for OCIO configuration

___Professional Dell Pentium II (266 MHz or faster), minimum 64 MB of RAM, 3.0 GB of Hard Drive available for OCIO configuration

Secondary Support

___As defined in OCIO non-standard workstation policy

Laptops

Primary Support

___Dell Pentium II (266 MHz or faster), minimum 64 MB of RAM, 3.0 GB of Hard Drive available for OCIO configuration

___Toshiba Pentium II (266 MHz or faster), minimum 64 MB of RAM, 3.0 GB of Hard Drive available for OCIO configuration

Secondary Support

___As defined in OCIO non-standard workstation policy

Printers

Primary Support

___HP LaserJet 5 and newer

Secondary Support

___HP LaserJet 4

Monitors

Primary Support

___17-inch or larger, capable of 1024x768 resolution

Personal Digital Assistants (PDA)

Primary Support

___Blackberry RIM 957

___Blackberry RIM 950

Secondary Support

___IntelliSync

___Microsoft ActiveSync 3.1 or newer

Software

Client Operating Systems

Primary Support

___Windows 2000 Professional Service Pack (SP)2

Secondary Support

___As defined in OCIO non-standard workstation policy

Office Suites

Primary Support

___Office 2000 Service Release (SR) 1A with Word 2000, Excel 2000, PowerPoint 2000, Access 2000

Anti-Virus Software

Primary Support

___Norton AntiVirus 2000 Corporate Edition 7.5

Communications

Primary Support

___Citrix ICA

Secondary Support

___Citrix Winframe

Terminal Emulation Software

Primary Support

___Attachmate 6.5

Database Clients

Primary Support

___Oracle 8.1.7 Client

___Microstrategy 7

Electronic Mail Software

Primary Support

___Outlook 2000

Internet Browsers

Primary Support

___Internet Explorer 5.5 SP1 (128-bit encryption)

Secondary Support

___Netscape 4.x

Helper Plug-Ins

Primary Support

___Adobe Acrobat Reader 5.0 and newer

___RealPlayer 8.0 Intranet

Project Management Software

Primary Support

___Microsoft Project 2000

___TeamMate 2000

Web/Desktop Publishing Software

Secondary Support

___Adobe Illustrator 7.0

___Adobe PageMaker 6.5 and newer

___Adobe Photoshop 5.0

___Interwoven LaunchPad

___Macromedia Dreamweaver 2.0 and newer

___Macromedia Fireworks 2.0 and newer

___Macromedia FreeHand 7.0

___Macromedia HomeSite 4.0

___NetViz 4.0

___Publisher 2000

Groupware

Secondary Support

___Lotus Notes Client (all versions)

Assistive Technology Software

Primary Support

___Aladdin Genie CCTV
___Dragon Systems NaturallySpeaking 4.0 and newer
___Freedom Scientific JAWS for Windows 3.7
___Gus Word Prediction
___IBM Homepage Reader 2.5 and newer
___NexCom 300 TTY modem, which requires an ISA slot
___NexTalk/NTS, NXI Communications NTS 3.41 and newer
___ZoomText Xtra Level 2 7.04 and newer

Secondary Support

___NXI Communications NexTalk for Windows
___WinTalk modem

Principal Office-Specialized Applications

Primary Support

___ARCHIBUS/FM-10
___CARS
___CCM Plus
___CMIS
___DACS
___EDCAPS
___EDICS
___Folio Builder 4.2
___Folio Views 4.2
___HEATWEB 3.11
___IAS
___Method/1 GuideVersion 11
___Monarch Professional 5.02
___Ombusman Case Tracking System 2.0
___Peer Review System
___TRAINS

Secondary Support

___CMTS
___DLOS
___Folio Views 3.11
___GAPS
___GPAS
___IEFARS
___OCR Electronic Library
___OSERS Quick
___PC Travel Drop Box
___PEPS
___PFIE
___Response Phone System
___SACONS
___Total Access Agent

Network Operating Systems and Enterprise Software

Primary Support

___Cisco IOS 12.1(5) (Router)
___Cisco IOS 6.1(2) and newer (Switch)
___Microsoft Exchange 5.5 SP4
___Microsoft SMS 2.0 SP3
___Microsoft NT Server 4.0 SP6a
___Microsoft Windows 2000 Server SP2

___Netscape Compass Server 3.0 (SPARC)
___Netscape Enterprise Server 3.51 (SPARC)
___Oracle 8.1.7
___Raptor Firewall with PowerVPN Version 6.5
___Solaris 2.6 (SPARC)
___SQL Server 7.0 SP5
___SQL Server 2000 SP1
___Terminal Server 4.0 SP6a

Secondary Support

___All versions of Linux
___All versions of Lotus Notes
___Microsoft Internet Information Server 4.0 and newer
___SQL Server 6.5